



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/669,399	09/23/2003	Scott Morris	9400-39	3957
39072 7590 06/25/2007 MYERS BIGEL SIBLEY & SAJOVEC, P.A. P.O. BOX 37428 RALEIGH, NC 27627			EXAMINER BAUM, RONALD	
			ART UNIT 2136	PAPER NUMBER
			MAIL DATE 06/25/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/669,399	Applicant(s) MORRIS ET AL.	
	Examiner Ronald Baum	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 19 April 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-54 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-54 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 23 September 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>9/23/2003</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This action is in reply to applicant's correspondence of 19 April 2007.
2. Claims 1-54 are pending for examination.
3. Claims 1-54 are rejected.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-54 are rejected under 35 U.S.C. 102(e) as being anticipated by Evans et al, U.S. Patent Application Publication US 2002/0171546 A1.

5. As per claim 1; "A method of resetting a password for a network service account, the method comprising:

redirecting the user to a password reset tool,

wherein the user is blocked from network access

other than the password reset tool while being redirected [*ABSTRACT, figures 3-6 and associated descriptions, para. 0005-0015, whereas the universal and customizable security system where the inputs are login/password entry functionality and biometric verification (i.e., redirected via the rules based*

routing to the appropriate processing element), such that the corresponding 'security actions in response' (via the associated rules) inclusive of 'reset passwords' (i.e., 'password reset tool'), network access/connectivity restriction (i.e., 'blocked from network access') as a function of password login/user verification, clearly encompasses the claimed limitations as broadly interpreted by the examiner.];

after redirecting the user to the password reset tool,

accepting user entry of verification information [ABSTRACT, figures 3-6 and associated descriptions, para. 0005-0015, whereas the login/password entry functionality and biometric verification (i.e., redirected via the rules based routing to the appropriate processing element), such that the corresponding 'security actions in response' (via the associated rules) inclusive of 'reset passwords' (i.e., 'password reset tool'), clearly encompasses the claimed limitations as broadly interpreted by the examiner.];

comparing

the verification information from the user with

known verification information for the user [ABSTRACT, figures 3-6 and associated descriptions, para. 0005-0015, whereas the login/password entry functionality and biometric verification (i.e., redirected via the rules based routing to the appropriate processing element), such that the corresponding 'security actions in response' (via the associated rules) inclusive of 'reset passwords' (i.e., 'password reset tool'), clearly encompasses the claimed limitations as broadly interpreted by the examiner.];

accepting user entry of a new password if

the verification information accepted from the user matches

the known verification information for the user [*ABSTRACT, figures 3-6 and associated descriptions, para. 0005-0015, whereas the login/password entry functionality and biometric verification (i.e., redirected via the rules based routing to the appropriate processing element), such that the corresponding 'security actions in response' (via the associated rules) inclusive of 'reset passwords' (i.e., 'password reset tool'), clearly encompasses the claimed limitations as broadly interpreted by the examiner.*]; and storing the new password as

the known password for the user [*ABSTRACT, figures 3-6 and associated descriptions, para. 0005-0015, whereas the login/password entry functionality and biometric verification (i.e., redirected via the rules based routing to the appropriate processing element), such that the corresponding 'security actions in response' (via the associated rules) inclusive of 'reset passwords' (i.e., 'password reset tool'), clearly encompasses the claimed limitations as broadly interpreted by the examiner.*].”.

As per claim 19, this claim is the system claim for the method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection.

As per claim 37, this claim is the embodied software claim for the method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection.

6. Claim 2 *additionally recites* the limitation that; “A method according to Claim 1 further comprising:

before redirecting the user to the password reset tool,
accepting entry of a password; and
before redirecting the user to the password reset tool,
comparing the entered password with a known password,
wherein redirecting the user to the password reset tool comprises
redirecting the user to the password reset tool if
the entered password does not match
the known password.”.

The teachings of Evans et al are directed towards such limitations (i.e., ABSTRACT, figures 3-6 and associated descriptions, para. 0005-0015, whereas the universal and customizable security system where the inputs are login/password entry functionality and biometric verification (i.e., redirected via the rules based routing to the appropriate processing element, post ‘biometric verification’ or password/login), such that the corresponding ‘security actions in response’ (via the associated rules) inclusive of redirection to the ‘reset passwords’ (i.e., ‘password reset tool’), functionality, clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

As per claim 20, this claim is the system claim for the method claim 2 above, and is rejected for the same reasons provided for the claim 2 rejection.

As per claim 38, this claim is the embodied software claim for the method claim 2 above, and is rejected for the same reasons provided for the claim 2 rejection.

7. Claim 3 *additionally recites* the limitation that; “A method according to Claim 2 wherein accepting entry of a password comprises
- accepting entry of the password at
- a first server, and
- wherein redirecting the user to a password reset tool comprises
- redirecting the user to
- a second server providing the password reset tool.”.

The teachings of Evans et al are directed towards such limitations (i.e., ABSTRACT, figures 3-6 and associated descriptions, para. 0005-0015, whereas the universal and customizable security system where the inputs are login/password entry functionality and biometric verification (i.e., redirected via the rules based routing to the appropriate processing element, post ‘biometric verification’ or password/login), such that the corresponding ‘security actions in response’ (via the associated rules) inclusive of redirection to the ‘reset passwords’ (i.e., ‘password reset tool’), functionality is configured as a system, inclusive of the Microsoft Windows™ network (i.e., LAN, client/server, P2P (multi-server), etc.,) environment, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

As per claim 21, this claim is the system claim for the method claim 3 above, and is rejected for the same reasons provided for the claim 3 rejection.

As per claim 39, this claim is the embodied software claim for the method claim 3 above, and is rejected for the same reasons provided for the claim 3 rejection.

8. Claim 4 *additionally recites* the limitation that; “A method according to Claim 2 wherein accepting entry of a password comprises
- accepting entry of the password from
- a remote electronic device.”.

The teachings of Evans et al are directed towards such limitations (i.e., ABSTRACT, figures 3-6 and associated descriptions, para. 0005-0015, whereas the universal and customizable security system where the inputs are login/password entry functionality and biometric verification (i.e., redirected via the rules based routing to the appropriate processing element, post ‘biometric verification’ or password/login), such that the corresponding ‘security actions in response’ (via the associated rules) inclusive of redirection to the ‘reset passwords’ (i.e., ‘password reset tool’), functionality is configured as a system, inclusive of the Microsoft Windows™ network (i.e., multi-node whereas at least 1 node of a multi-node LAN, client/server, P2P, etc., is clearly remote) environment, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

As per claim 22, this claim is the system claim for the method claim 4 above, and is rejected for the same reasons provided for the claim 4 rejection.

As per claim 40, this claim is the embodied software claim for the method claim 4 above, and is rejected for the same reasons provided for the claim 4 rejection.

9. Claim 5 *additionally recites* the limitation that; “A method according to Claim 4 wherein accepting user entry of the password from a remote electronic device comprises accepting entry of the password from the remote electronic device over a telephone line.”.

The teachings of Evans et al are directed towards such limitations (i.e., ABSTRACT, figures 3-6 and associated descriptions, para. 0005-0015, whereas the universal and customizable security system where the inputs are login/password entry functionality and biometric verification (i.e., redirected via the rules based routing to the appropriate processing element, post ‘biometric verification’ or password/login), such that the corresponding ‘security actions in response’ (via the associated rules) inclusive of redirection to the ‘reset passwords’ (i.e., ‘password reset tool’), functionality is configured as a system, inclusive of the Microsoft Windows™ network (i.e., multi-node whereas at least 1 node of a multi-node LAN, client/server, P2P, etc., is clearly remote, and communications is inclusive of Internet/modem (i.e., ‘... telephone line’)) environment, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

As per claim 23, this claim is the system claim for the method claim 5 above, and is rejected for the same reasons provided for the claim 5 rejection.

As per claim 41, this claim is the embodied software claim for the method claim 5 above, and is rejected for the same reasons provided for the claim 5 rejection.

10. Claim 6 *additionally recites* the limitation that; “A method according to Claim 2 further comprising:

providing network service for the user

without redirecting to the password reset tool if

the entered password matches

the known password for the user.”.

The teachings of Evans et al are directed towards such limitations (i.e., ABSTRACT, figures 3-6 and associated descriptions, para. 0005-0015, whereas the universal and customizable security system where the inputs are login/password entry functionality and biometric verification (i.e., redirected via the rules based routing to the appropriate processing element), such that the corresponding ‘security actions in response’ (via the associated rules) inclusive of ‘reset passwords’ (i.e., ‘password reset tool’), network access (i.e., ‘providing network service’)/connectivity restriction as a function of password login/user verification, clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

As per claim 42, this claim is the embodied software claim for the method claim 6 above, and is rejected for the same reasons provided for the claim 6 rejection.

11. Claim 7 *additionally recites* the limitation that; “A method according to Claim 2 wherein

redirecting the user to a password reset tool comprises
redirecting the user to the password reset tool if
a predetermined number of passwords
have been accepted from the user during a session
without matching the known password.”.

The teachings of Evans et al are directed towards such limitations (i.e., ABSTRACT, figures 3-6 and associated descriptions, para. 0005-0015, whereas the universal and customizable security system where the inputs are login/password entry functionality and biometric verification (i.e., redirected via the rules based routing to the appropriate processing element, inclusive of dependence on failed login attempts, post predetermined number of attempts/ predetermined login time), such that the corresponding ‘security actions in response’ (via the associated rules) inclusive of redirection to the ‘reset passwords’ (i.e., ‘password reset tool’), functionality, clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

As per claim 43, this claim is the embodied software claim for the method claim 7 above, and is rejected for the same reasons provided for the claim 7 rejection.

12. Claim 8 *additionally recites* the limitation that; “A method according to Claim 2 wherein accepting user entry of a password further comprises
accepting user entry of
a username and
the password, and

wherein redirecting the user to a password reset tool if the password from the user does not match the known password further comprises

redirecting the user to the password reset tool only if

the username entered by the user is

a valid username.”.

The teachings of Evans et al are directed towards such limitations (i.e., ABSTRACT, figures 3-6 and associated descriptions, para. 0005-0015, whereas the universal and customizable security system where the inputs are login (inclusive of user name/identification)/password entry functionality/verification (i.e., redirected via the rules based routing to the appropriate processing element, post ‘biometric verification’ or password/login), such that the corresponding ‘security actions in response’ (via the associated rules) inclusive of redirection to the ‘reset passwords’ (i.e., ‘password reset tool’), functionality, clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

As per claim 26, this claim is the system claim for the method claim 8 above, and is rejected for the same reasons provided for the claim 8 rejection.

As per claim 44, this claim is the embodied software claim for the method claim 8 above, and is rejected for the same reasons provided for the claim 8 rejection.

13. Claim 9 *additionally recites* the limitation that; “A method according to Claim 1 further comprising:

terminating redirecting of the user to the password reset tool if
the verification information entered by the user does not match
the known verification information.”.

The teachings of Evans et al are directed towards such limitations (i.e., ABSTRACT, figures 3-6 and associated descriptions, para. 0005-0015, whereas the universal and customizable security system where the inputs are login/password entry functionality and biometric verification (i.e., redirected/not redirected (‘terminating redirecting ...’) via the rules based routing to the appropriate processing element), such that the corresponding ‘security actions in response’ (via the associated rules) inclusive of password reset tool access or not, as a function of password login/user verification, clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

As per claim 27, this claim is the system claim for the method claim 9 above, and is rejected for the same reasons provided for the claim 9 rejection.

As per claim 45, this claim is the embodied software claim for the method claim 9 above, and is rejected for the same reasons provided for the claim 9 rejection.

14. Claim 10 *additionally recites* the limitation that; “A method according to Claim 1 further comprising:

terminating redirecting of the user to the password reset tool if
user verification information is accepted

a predetermined number of times without matching
the known verification information.”.

The teachings of Evans et al are directed towards such limitations (i.e., ABSTRACT, figures 3-6 and associated descriptions, para. 0005-0015, whereas the universal and customizable security system where the inputs are login/password entry functionality and biometric verification (i.e., redirected/not redirected (‘terminating redirecting ...’) via the rules based post predetermined number of attempts), such that the corresponding ‘security actions in response’ (via the associated rules) inclusive of redirection to the ‘reset passwords’ (i.e., ‘password reset tool’), functionality, clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

As per claim 28, this claim is the system claim for the method claim 10 above, and is rejected for the same reasons provided for the claim 10 rejection.

As per claim 46, this claim is the embodied software claim for the method claim 10 above, and is rejected for the same reasons provided for the claim 10 rejection.

15. Claim 11 *additionally recites* the limitation that; “A method according to Claim 1 further comprising:

terminating redirecting of the user to the password reset tool if
a predetermined period of time passes without accepting
user verification information matching

the known verification information.”.

The teachings of Evans et al are directed towards such limitations (i.e., ABSTRACT, figures 3-6 and associated descriptions, para. 0005-0015, whereas the universal and customizable security system where the inputs are login/password entry functionality and biometric verification (i.e., redirected/not redirected (‘terminating redirecting ...’) via the rules based post predetermined login time), such that the corresponding ‘security actions in response’ (via the associated rules) inclusive of redirection to the ‘reset passwords’ (i.e., ‘password reset tool’), functionality, clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

As per claim 29, this claim is the system claim for the method claim 11 above, and is rejected for the same reasons provided for the claim 11 rejection.

As per claim 47, this claim is the embodied software claim for the method claim 11 above, and is rejected for the same reasons provided for the claim 11 rejection.

16. Claim 12 *additionally recites* the limitation that; “A method according to Claim 1 further comprising:

after accepting entry of the new password,

terminating redirecting of the user to the password reset tool.”.

The teachings of Evans et al are directed towards such limitations (i.e., ABSTRACT, figures 3-6 and associated descriptions, para. 0005-0015, whereas the universal and customizable security system where the inputs are login/password entry functionality and biometric verification (i.e.,

redirected/not redirected ('terminating redirecting ...') via the rules based post accepting entry of the new password), such that the corresponding 'security actions in response' (via the associated rules) inclusive of redirection to the 'reset passwords' (i.e., 'password reset tool'), functionality, clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

As per claim 30, this claim is the system claim for the method claim 12 above, and is rejected for the same reasons provided for the claim 12 rejection.

As per claim 48, this claim is the embodied software claim for the method claim 12 above, and is rejected for the same reasons provided for the claim 12 rejection.

17. Claim 13 *additionally recites* the limitation that; "A method according to Claim 1 further comprising:

after accepting entry of the new password from a remote electronic device,
transmitting instructions for the remote electronic device
to automatically save the new password."

The teachings of Evans et al are directed towards such limitations (i.e., ABSTRACT, figures 3-6 and associated descriptions, para. 0005-0015, whereas the universal and customizable security system where the inputs are login/password entry functionality and biometric verification (i.e., redirected/not redirected ('terminating redirecting ...') via the rules based post accepting entry of the new password), such that the corresponding 'security actions in response' (via the associated rules) inclusive of the passwords storage functionality, is configured as a system, inclusive of the

Microsoft Windows™ network (i.e., multi-node whereas at least 1 node of a multi-node LAN, client/server, P2P, etc., is clearly remote) environment, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

As per claim 31, this claim is the system claim for the method claim 13 above, and is rejected for the same reasons provided for the claim 13 rejection.

As per claim 49, this claim is the embodied software claim for the method claim 13 above, and is rejected for the same reasons provided for the claim 13 rejection.

18. Claim 14 *additionally recites* the limitation that; “A method according to Claim 1 wherein

redirecting the user to the password reset tool comprises

tunneling the user to the password reset tool.”.

The teachings of Evans et al are directed towards such limitations (i.e., ABSTRACT, figures 3-6 and associated descriptions, para. 0005-0015, whereas the universal and customizable security system where the inputs are login/password entry functionality and biometric verification (i.e., redirected/not redirected (‘terminating redirecting ...’) via the rules based post accepting entry of the new password), such that the corresponding ‘security actions in response’ (via the associated rules) inclusive of the passwords storage functionality, is configured as a system, inclusive of the Microsoft Windows™ network (i.e., and associated VPN (‘tunneling the ...’) configurability)

environment, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

As per claim 32, this claim is the system claim for the method claim 14 above, and is rejected for the same reasons provided for the claim 14 rejection.

As per claim 50, this claim is the embodied software claim for the method claim 14 above, and is rejected for the same reasons provided for the claim 14 rejection.

19. Claim 15 *additionally recites* the limitation that; “A method according to Claim 1 further comprising:

after redirecting the user to the password reset tool,
accepting a request for a network browser; and
responsive to accepting the request for an network browser,
providing a password reset window including
prompts for entry of
the verification information.”.

The teachings of Evans et al are directed towards such limitations (i.e., ABSTRACT, figures 3-6 and associated descriptions, para. 0005-0015, whereas the universal and customizable security system where the inputs are login/password entry functionality and biometric verification (i.e., redirected via the rules based post accepting entry of the new password via the GUI (‘browser’)), such that the corresponding ‘security actions in response’ (via the associated rules) inclusive of

the passwords storage functionality, is configured as a system, inclusive of the Microsoft Windows™ network configurability) environment, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

As per claim 33, this claim is the system claim for the method claim 15 above, and is rejected for the same reasons provided for the claim 15 rejection.

As per claim 51, this claim is the embodied software claim for the method claim 15 above, and is rejected for the same reasons provided for the claim 15 rejection.

20. Claim 16 *additionally recites* the limitation that; “A method according to Claim 1 further comprising:

after redirecting the user to the password reset tool,
accepting a request for e-mail service; and
responsive to accepting the request for e-mail service,
providing a password reset e-mail including
a link to a password reset window including
prompts for entry of
the verification information.”.

The teachings of Evans et al are directed towards such limitations (i.e., ABSTRACT, figures 3-6 and associated descriptions, para. 0005-0015, whereas the universal and customizable security system where the inputs are login/password entry functionality and biometric verification (i.e.,

redirected via the rules), such that the corresponding 'security actions in response' (via the associated rules) inclusive of the enable or disable e-mail functionality, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

As per claim 34, this claim is the system claim for the method claim 16 above, and is rejected for the same reasons provided for the claim 16 rejection.

As per claim 52, this claim is the embodied software claim for the method claim 16 above, and is rejected for the same reasons provided for the claim 16 rejection.

21. Claim 17 *additionally recites* the limitation that; "A method according to Claim 16 further comprising:

responsive to accepting the request for e-mail,
blocking access to all e-mails other than
the password reset e-mail.".

The teachings of Evans et al are directed towards such limitations (i.e., ABSTRACT, figures 3-6 and associated descriptions, para. 0005-0015, whereas the universal and customizable security system where the inputs are login/password entry functionality and biometric verification (i.e., redirected via the rules), such that the corresponding 'security actions in response' (via the associated rules) inclusive of the enable or disable e-mail functionality, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

As per claim 35, this claim is the system claim for the method claim 17 above, and is rejected for the same reasons provided for the claim 17 rejection.

As per claim 53, this claim is the embodied software claim for the method claim 17 above, and is rejected for the same reasons provided for the claim 17 rejection.

22. Claim 18 *additionally recites* the limitation that; “A method according to Claim 1 wherein

the network service account comprises

an Internet service account.”.

The teachings of Evans et al are directed towards such limitations (i.e., ABSTRACT, figures 3-6 and associated descriptions, para. 0005-0015, whereas the universal and customizable security system where the inputs are login/password entry functionality and biometric verification (i.e., redirected via the rules), such that the corresponding ‘security actions in response’ (via the associated rules) inclusive of the Internet connectivity functionality, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

As per claim 36, this claim is the system claim for the method claim 18 above, and is rejected for the same reasons provided for the claim 18 rejection.

As per claim 54, this claim is the embodied software claim for the method claim 18 above, and is rejected for the same reasons provided for the claim 18 rejection.

Conclusion

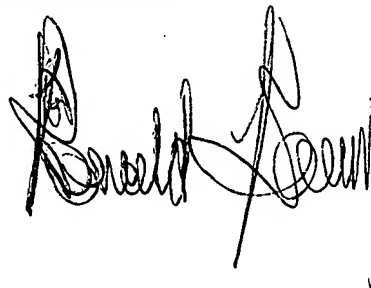
23. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861 and unofficial email is Ronald.baum@uspto.gov. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at (571) 272-4195. The Fax number for the organization where this application is assigned is **571-273-8300**.

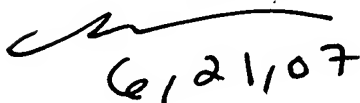
Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ronald Baum

Patent Examiner

A handwritten signature in black ink, appearing to read 'Ronald Baum', with a stylized, cursive script.

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

A handwritten signature in black ink, appearing to read 'Nasser Moazzami', with a stylized, cursive script.

6/21/07